WHAT IS CLAIMED IS:

1. A tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal, comprising:

band division means for dividing said digital image signal into a plurality of frequency bands;

authentication data generation means for generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series;

key data embedding means for embedding said key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands;

authentication data embedding means for embedding said authentication data in transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands; and

band synthesis means for reconstructing the digital image signal in which the information has been embedded by using said MRA and said MRR to which data embedding processing is subjected.

2. The tamper-detection-information embedding apparatus according to claim 1, wherein

a set value T (T is a positive integer) and a set value m (m is an integer not more than T) are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size, and

said authentication data embedding means embeds said authentication data in each transform coefficient of said MRR by comparing an absolute value of said transform coefficient with said set value T, and if the absolute value is less than said set value T, setting the transform coefficient to said set value +m or -m depending on a bit value of said authentication data to be embedded, and if the absolute value is not less than said set value T, setting the transform coefficient to an even or odd integer nearest to said value q depending on the bit value of said authentication data to be embedded.

3. A tamper detecting apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal, comprising:

band division means for dividing said digital image signal into a plurality of frequency bands;

key data extraction means for extracting key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands;

authentication data generation means for generating a pseudo-random number series by using said key data, and generating authentication data from the pseudo-random number series;

embedded information extraction means for extracting embedded information embedded based on said key data by said specific apparatus from transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands; and

tamper determination means for comparing said embedded information with said authentication data for verification and determining whether said digital image has been tampered with.

4. The tamper detecting apparatus according to claim 3, wherein

said tamper determination means comprises:

block division means for dividing the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

regional embedded information read means for reading, for each of said unit blocks, embedded information embedded in the transform coefficients of said MRR that represents the same spatial region as the unit block, serially from all of said embedded information extracted by said embedded information extraction means;

regional authentication data read means for reading, for each of said unit blocks, authentication data corresponding in position to said embedded information serially read by said regional embedded information read means, serially from all of said authentication data generated by said authentication data generation means; and

block-tamper determination means for comparing said embedded information serially read with said authentication data serially read and determining, for each of said unit blocks, whether said digital image has been tampered with.

5. The tamper detecting apparatus according to claim 3, wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient is by a predetermined quantization step size and then rounding off the result, and

said embedded information extraction means extracts said embedded information from each transform coefficient of said MRR by comparing an absolute value of said transform coefficient with said set value T, and if the absolute value is less than said set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and if the absolute value is not less than said set value T, determining whether said value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination.

6. The tamper detecting apparatus according to claim 4, wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result, and

said embedded information extraction means extracts said embedded information from each transform coefficient of said MRR by comparing an absolute value of said transform coefficient with said set value T, and if the absolute value is less than said set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and if the absolute value is not less than said set value T, determining whether said value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination.

7. A tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal, comprising:

a step of dividing said digital image signal into a plurality of frequency bands;

a step of generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series;

a step of embedding said key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands;

a step of embedding said authentication data in transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands; and

a step of reconstructing the digital image signal in which the information has been embedded by using said MRA and said MRR to which data embedding processing is subjected.

8. The tamper-detection-information embedding method according to claim 7, wherein

a set value T (T is a positive integer) and a set value m (m is an integer not more than T) are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size, and

said step of embedding authentication data includes:

a step of comparing an absolute value of said transform coefficient with said set value T;

a step of setting the transform coefficient to said set value +m or -m depending on a bit value of said authentication data to be embedded if the absolute value is less than said set value T; and

a step of setting the transform coefficient to an even or odd integer nearest to said value q depending on the bit value of said authentication data to be embedded if the absolute value is not less than said set value T.

9. A tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal, comprising:

a step of dividing said digital image signal into a plurality of frequency bands;

a step of extracting key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands;

a step of generating a pseudo-random number series by using said key data, and generating authentication data from the pseudo-random number series;

a step of extracting embedded information embedded based on said key data by said specific apparatus from transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands; and

a step of comparing said embedded information with said authentication data for verification and determining whether said digital image has been tampered with.

10. The tamper detecting method according to claim 9, wherein

said step of determining tamper comprises:

a step of dividing the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

a step of reading, for each of said unit blocks, embedded information embedded in the transform coefficients of said MRR that represents the same spatial region as the unit block, serially from all of said embedded information;

a step of reading, for each of said unit blocks, authentication data corresponding in position to said embedded information serially read, serially from all of said authentication data; and

a step of comparing a series of said embedded information serially read with a series of said authentication data serially read and determining, for each of said unit blocks, whether said digital image has been tampered with.

11. The tamper detecting method according to claim 9, wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result, and

said step of extracting embedded information includes:

a step of comparing an absolute value of said transform coefficient with said set value T;

a step of determining whether a value of the transform coefficient is positive or negative if the absolute value is less than said set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination;

a step of determining whether said value q is even or odd if the absolute value is not less than said set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination.

12. The tamper detecting method according to claim 10, wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result, and

said step of extracting embedded information includes:

a step of comparing an absolute value of said transform coefficient with said set value T;

a step of determining whether a value of the transform coefficient is positive or negative if the absolute value is less than said set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination;

a step of determining whether said value q is even or odd if the absolute value is not less than said set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination.

13. A recording medium on which a program to be run on a computer device is recorded for carrying out a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal, the method comprising the steps of:

dividing said digital image signal into a plurality of frequency bands;

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series;

embedding said key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands;

embedding said authentication data in transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands; and

reconstructing the digital image signal in which the information has been embedded by using said MRA and said MRR to which data embedding processing is subjected.

14. The recording medium according to claim 13, wherein

a set value T (T is a positive integer) and a set value m (m is an integer not more than T) are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size, and

said step of embedding authentication data includes the steps of:

comparing an absolute value of said transform coefficient with said set value T;

setting the transform coefficient to said set value +m or -m depending on a bit value of said authentication data to be embedded if the absolute value is less than said set value T; and

setting the transform coefficient to an even or odd integer nearest to said value q depending on the bit value of said authentication data to be embedded if the absolute value is not less than said set value T.

15. A recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on

tamper-detection-information embedded by a specific apparatus in a digital image signal, the method comprising the steps of:

dividing said digital image signal into a plurality of frequency bands;

extracting key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands;

generating a pseudo-random number series by using said key data, and generating authentication data from the pseudo-random number series;

extracting embedded information embedded based on said key data by said specific apparatus from transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands; and

comparing said embedded information with said authentication data for verification and determining whether said digital image has been tampered with.

16. The recording medium according to claim 15, wherein said step of determining tamper comprises the steps of:

dividing the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

reading, for each of said unit blocks, embedded information embedded in the transform coefficients of said MRR that represents the same spatial region as the unit block, serially from all of said embedded information;

reading, for each of said unit blocks, authentication data corresponding in position to said embedded information serially read, serially from all of said authentication data; and

comparing a series of said embedded information serially read with a series of said authentication data serially read and determining, for each of said unit blocks, whether said digital image has been tampered with.

17. The recording medium according to claim 15, wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient is divided by a predetermined quantization step size and then rounding off the result, and

said step of extracting embedded information includes the steps of:

comparing an absolute value of said transform coefficient with said set value T;

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than said set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination;

determining whether said value q is even or odd if the absolute value is not less than said set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination.

18. The recording medium according to claim 16, wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result, and

said step of extracting embedded information includes the steps of:

comparing an absolute value of said transform coefficient with said set value T;

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than said set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination;

determining whether said value q is even or odd if the absolute value is not less than said set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination.